Overview

- Over the past few weeks, there has been considerable speculation in the press about two NSA programs as a result of unauthorized disclosures of classified information.

    - One program, authorized by Section 215 of the USA Patriot Act, concerns the collection only of telephony metadata, such as telephone numbers dialed and length of calls, and is designed to address a seam between foreign and domestic counterterrorism efforts exposed in the 9/11 attacks.

    - The second program, authorized under Section 702 of the FISA Amendments Act, concerns the targeting of communications of non-U.S. persons located abroad for foreign intelligence purposes, like counterterrorism and counterproliferation.

- This speculation has been fueled by incomplete and inaccurate information, with little context as to the purpose of these programs, their value to our national security and that of our allies, and the protections that are in place to preserve our privacy and civil liberties.

- These programs are distinct but complementary. In recent years, the intelligence gathered under them has contributed to the disruption of dozens of potential terrorist plots here in the homeland and in more than 20 countries around the world. We are working to be able to provide more information about this.

- Both of these programs were authorized by Congress on a bipartisan basis, are approved by the Foreign Intelligence Surveillance Court, and are rigorously and regularly reviewed by the Department of Justice and Office of the Director of National Intelligence.

Section 215 of the Patriot Act

- This program is about metadata; it does not allow the government to listen to anyone's phone calls. The information acquired does not contain the content of any communications, the identity of any party to the communication, or any cell phone locational information.

- The government does not indiscriminately sift through the telephony metadata acquired under this program. This program was specifically developed to allow the USG to detect communications between terrorists who are operating outside the US but who are communicating with potential operatives inside the US, a gap highlighted by the attacks of 9/11. The metadata acquired and stored under this program may be queried only when there is a reasonable suspicion, based on specific and articulated facts, that an identifier is associated with specific foreign terrorist organizations. In 2012, less than 300 unique identifiers met this standard and were queried.

- Only a very small fraction of the metadata acquired under the program is ever reviewed because the vast majority of it will never be responsive to a terrorism-related query.

- The program is subject to strict controls and oversight: the metadata is segregated and queries against the database are documented and audited. Only a small number of specifically-trained officials may access the data; the Foreign Intelligence Surveillance Court reviews the program every 90 days; and the data must be destroyed within 5 years.

Section 702 of the FISA Amendments Act

- This program does not allow the government to target the phone calls or emails of any U.S. citizen or any other U.S. person anywhere in the world, or any person known to be in the United States. It only allows targeting of communications of foreigners, and even then only when those communications may have foreign intelligence value.

- Congress requires the Government to develop and obtain judicial approval for "minimization" procedures to ensure appropriate protection of any information about U.S. persons that may be incidentally acquired. The Government did that, and its procedures were approved by the Foreign Intelligence Surveillance Court.

- The program is subject to strict controls and oversight: targeting decisions and the Government's use of the acquired information are regularly reviewed by the Department of Justice and the Office of the Director of National Intelligence; semiannual reports are provided to Congress and the Foreign Intelligence Surveillance Court; and the Foreign Intelligence Surveillance Court must renew the program each year upon certification by the Attorney General and the Director of National Intelligence.

- Within this regime of strict controls and oversight, the USG requires (in legal terms, "compels") US technology companies to provide certain communications records. While required to comply, US companies have put energy, focus and commitment to consistently protect the privacy of their customers, as well as the safety and security of these same customers, around the world.

Value of These Authorities: NYC Attack Plot 2009

- The USG used these two authorities to help prevent a major al-Qa'ida directed attack on the Homeland.

    - In September 2009, using collection under Section 702 to monitor al-Qa'ida terrorists in Pakistan, NSA discovered that one of the Pakistani terrorists was in contact with an unknown person located in the US about efforts to procure explosive material. NSA

immediately tipped this information to the FBI, which investigated further, and identified the al-Qa'ida contact as Colorado-based extremist Najibullah Zazi.

- NSA and FBI worked together to determine the extent of Zazi's relationship with al-Qa'ida and to identify any other foreign or domestic terrorist links. NSA received Zazi's telephone number from FBI and ran it against the Section 215 Business Records data, identifying and passing additional leads back to the FBI for investigation. One of these leads revealed a previously unknown number for co-conspirator Adis Medunjanin and corroborated his connection to Zazi as well as to other US-based extremists.

- The FBI investigated these leads, tracking Zazi as he traveled to meet up with his co-conspirators in New York, where they were planning to conduct a terrorist attack. Zazi and his co-conspirators were subsequently arrested, and the attack thwarted. Upon indictment, Zazi pled guilty to conspiring to bomb the NYC subway system. This plot was characterized as 'the most serious terrorist threat on US soil since 9/11.' In November 2012, Medunjanin was sentenced to life in prison.

- This success was just one of many in which we've leveraged the combined authorities of these programs, as well as others, to protect the American people. While the operational details behind the many other disruptions must remain secret to allow us to continue to effectively leverage our capabilities in the face of those who still aspire to do great harm to our citizens and our allies, we believe it is absolutely critical that the American people have faith and confidence in how we are using the authorities granted to us to keep them safe.

- While debates may go on about the proper balance between securing our nation and safeguarding the privacies and liberties which we all hold so dear, the American people deserve to understand what we are doing to protect both.